UB3.0.2.5:SAM1.0

Defense Information Infrastructure (DII)
Common Operating Environment (COE)

System Administrator=s Manual

Unified Build 3.0.2.5

(TMS/UCP)

14 April 1997

Prepared for:

Defense Information Systems Agency (DISA)

Prepared by:

Inter-National Research Institute, Inc. (INRI)
10101 Old Grove Road
San Diego, CA 92131

Table of Contents

Notes

Introduction

The *Unified Build System Administrator's Manual* describes the system administration utilities included in the TMS/UCP segment and available from the TMS/UCP pull-down menu on the System Administrator menubar.

This manual also includes general communications information and troubleshooting techniques.

Notes

TMS/UCP System Administration Utilities

These options are located on the TMS/UCP pull-down menu. Some options may be located on a cascading menu. All options are described in this section in alphabetical order.

Availability of specific menu options depends upon two criteria:

- the platform (TAC-3/4 or Sparc 10/20)
- the access assigned to the user account profile

Archive TMS Data

Use this option to back up onto tape the current TMS files. The user may select all data for backup, or choose specific information; for example tracks, overlays, and PIM tracks only.

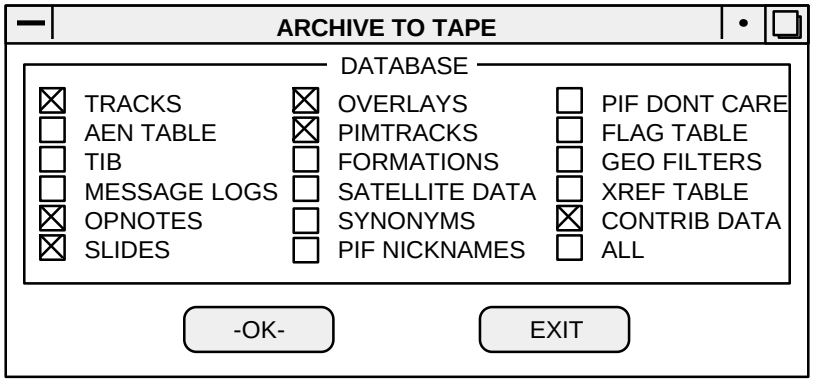
Important:

- Use a blank tape or a tape that can be overwritten.

  Remember, any information on the tape will be erased during backup.

- Do not overwrite the operating system or segment tapes supplied with the system. These tapes can reinstall the software in case of a fatal system crash.
- Once data is archived, write-protect the tape closing the lever on the top edge of the tape.

To access this window: TMS menu **:** DATABASE menu **:** ARCHIVE TMS DATA option.



> To archive data:

1. **Insert** a tape that is not write-protected.
2. **Select** ARCHIVE TMS DATA.
   - Rewinding the tape can take several minutes.
   - When the tape is positioned, the ARCHIVE TO TAPE window appears. The files displayed depend upon the installed software version.

3. **Toggle on** the checkboxes for the data to back up. A pop-up menu is available with SELECT ALL and UNSELECT ALL options.

    - If the ALL checkbox is toggled on, the only option available when the tape is restored is ALL.
    - If all checkboxes are toggled individually, or if SELECT ALL is chosen from the pop-up menu, the user may select which data files to restore.

4. **Click** OK.

    - When the process is complete, the tape is automatically rewound and the SYSTEM ADMINISTRATOR screen appears.

5. **Remove** the tape.

6. **Write-protect** the tape.

7. **Label** the tape "TMS DATA BACKUP." Include the date, version, and classification.

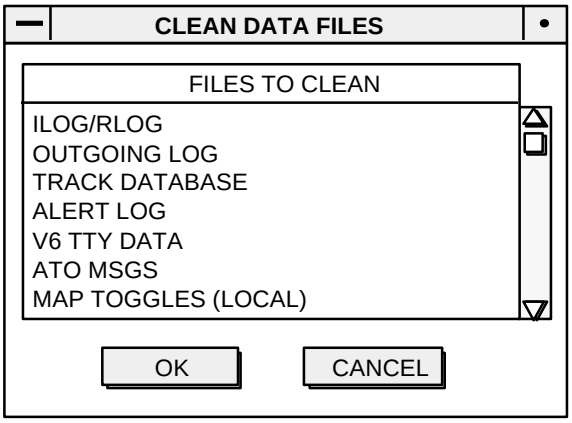
Clean Datafiles

This option deletes data files from the system. When selected on the server, many data types can be deleted, including *all* track information. When selected from another machine, *only* the MAP TOGGLES file can be deleted.

Use this option to:

- Clear classified information from the system.
- Clean the local MAP TOGGLES if the display is corrupted.

To access this window: DATABASE menu**:** CLEAN DATA FILES option.



> To clean data files:

1. **Highlight** the files to be cleaned.
2. **Click** OK to erase them, or click CANCEL to discontinue the process.
    - For example, if the TRACK DATABASE files were selected, all tracks except OWNTRACK would be removed from the tactical display when the system was restarted.

Config DDN Host Table

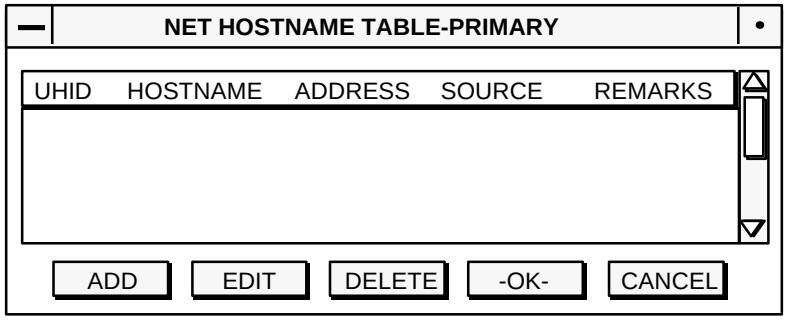
Use this option to configure and store a list of hostnames for a Network comms channel.

The CONFIG DDN HOST TABLE option can store two host tables:

- Primary: list of sites used during normal operations.
- Alternate: back-up list of sites.

A generic host table is established during installation. The System Administrator can edit this table to create a hostname list or create new entries using the ADD function. Each entry in the hostname list must have a unique IP address, name, and Unique Host Identification (UHID).

To access this window: COMMS **:** CONFIG DDN HOST TABLE option.



NET HOSTNAME TABLE Window Actions

> ADD—a new site to the hostname table.

1. Click ADD to open the ADD HOSTNAME window.
2. Enter the site's UHID, hostname, address, and remarks.
3. Toggle INTERNAL checkbox ON or OFF (described in *Internal Checkbox*).
4. Click OK to add the site, or CANCEL to discard.

> ALTERNATE (pop-up option)—shows alternate hostname list.

> ARCHIVE (pop-up option)—host table to clipboard.

- Use ARCHIVE-RESTORE from the MISC menu to archive list from the clipboard to tape.

> CANCEL—close the net hostname window without saving changes.

> Configure—the DDN Host Table:

1. Add or edit entries for the primary host list.
2. Select SET PRIMARY from the pop-up menu to define the primary list.
3. Select SET ALTERNATE to create an identical backup list.
4. Select PRIMARY from the pop-up menu to recall the primary list.
5. Click OK to save the configuration and close the window.

> DELETE—a site from the list.

> EDIT—a site's UHID, hostname, address, remarks, or internal/external flag.

> OK— to store the new configuration.

> PRIMARY (pop-up option)—show primary hostname list.

> PRINT (pop-up option)—a hard copy of hostname list.

> RESTORE (pop-up option)—hostname list from clipboard.

- Use ARCHIVE-RESTORE from the MISC menu to restore list from tape.)

> SELECT ALL (pop-up option)—names in the list.

> SET ALTERNATE (pop-up option)—designate current list as alternate hostname list.

> SET PRIMARY (pop-up option)—designate current list as primary hostname list.

> UNSELECT ALL (pop-up option)—names in the list.

> UPDATE (pop-up option)—show default hostname list installed with the software.

NET HOSTNAME TABLE Window Fields:

UHID
A unique three-character code that identifies the host. Each entry in the list must be assigned a UHID.

HOSTNAME
Full name of the host; each name must be unique.

ADDRESS
IP address of the host machine.

SOURCE
Internal or external to the site.

REMARKS
Remarks about the host name.

Internal Checkbox

The INTERNAL checkbox is used primarily by a WAN broadcast on the AntiDrug Network (ADNET). Sites on ADNET are designated either a Regional Coordinator (RC) or local site.

- An RC is responsible for sending track updates to its own local sites and other RCs.

  Its own local sites are marked as INTERNAL (checkbox toggled ON)

  Other entries are EXTERNAL (checkbox toggled OFF).

- A local site is responsible for sending updates only to its own RC.

  Its own RC is marked INTERNAL.

  Other entries are EXTERNAL.

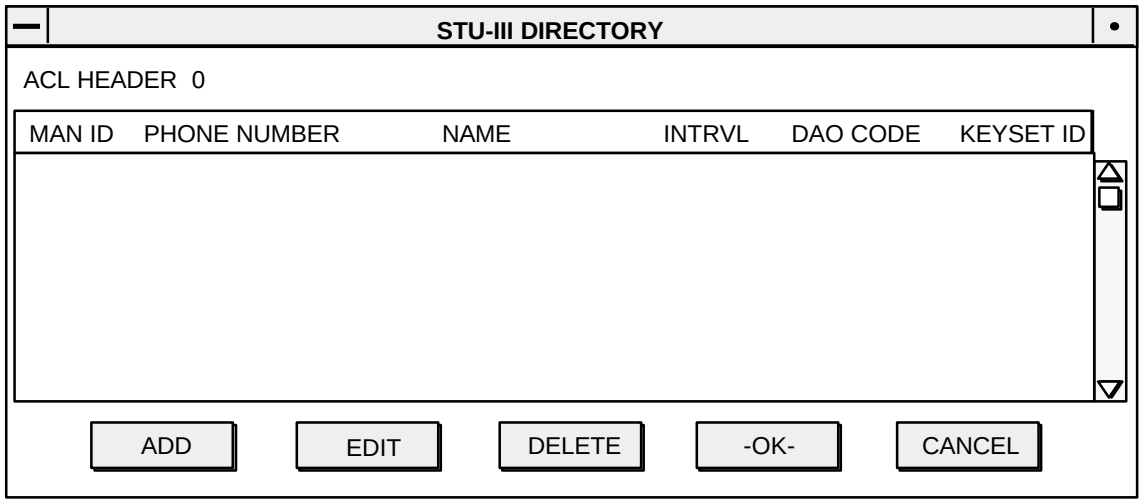
- The WAN broadcast uses the internal/external flag to route updates appropriately.

Config STU III Dir

Use this option to:

- Create and maintain a list of STU III recipients.
- Download the list of recipients to the Access Control List (ACL) of the sending STU III, using the DOWNLOAD ACL pop-up menu option.

To access this window: COMMS menu **:** CONFIG STU III DIR option.



In a networked environment, the server must be online before entries can be made in the STU III DIRECTORY. Otherwise, entries will be discarded and replaced by the existing master directory.

STU III DIRECTORY Window Actions

> ADD—a recipient.

1. **Click** ADD to open the ADD STU ENTRY window.
2. **Enter** a three-character ID.
3. **Enter** the phone number.
   - If there is an extension for the STU III, commas can create a pause between the phone number and the extension. The more commas, the longer the pause.
4. **Enter** the name of the organization.

5. **Enter** the call-back interval.

    - This option is used only with auto-answer, auto-secure SACS STU IIIs.

6. **Enter** the DAO code for the recipient.

    - This field is optional and can only be used with auto-answer, auto-secure SACS STU IIIs.
    - To use SACS STU IIIs in a closed network where no DAO code has been assigned, use a keyset ID instead.

7. **Enter** the keyset ID.

    - Each STU III may have as many as four keysets.
    - This field is optional and can only be used with auto-answer, auto-secure SACS STU IIIs.

8. **Click** OK to accept the entries, or click CANCEL to discard.

> ARCHIVE (pop-up option)—the list.

> CANCEL—discard changes and close window.

> DELETE—recipients.

1. **Select** one or more recipients from the scroll list.

2. **Click** DELETE.

> DOWNLOAD ACL (pop-up option)—Download the list of recipients to the Access Control List in the STU III.

1. **Turn on** the STU III.

2. **Change** the mode to accept the ACL download. (Refer to the STU III's user documentation.)

3. **Enter** a number in the ACL HEADER field (STU III DIRECTORY window).

    - Some devices accept any number; for example, the number 1.
    - Refer to the STU III's user documentation for the specific number of the device.

4. **Highlight** "automatic" recipients on the list.

5. **Select** DOWNLOAD ACL from the pop-up menu. The SELECT STU CHANNEL DEVICE window appears.

6. **Highlight** the STU III that will transmit messages.

7. **Click** OK to accept the entry, or click cancel to discontinue the process. A window appears confirming the preparation for the download.

8. **Click** OK to continue. If the download has been accepted, a window appears notifying the user that the process is complete.

9. **Click** OK to return to the STU III DIRECTORY window.

> EDIT—a recipient.

1. **Select** the organization from the scroll list.

2. **Click** EDIT to make changes.

3. **Click** OK to accept the changes or click CANCEL to discard.

> OK—accept changes and close window.

> PRINT (pop-up option)—Print the complete list of STU III recipients stored in the system. This option is not active in the current version of the software.

> RESTORE (pop-up option)—list from archive.

> SELECT ALL (pop-up option)—recipients in the list.

> UNSELECT ALL (pop-up option)—recipients in the list.

STU III DIRECTORY Window Fields

MAN ID
Indicates a manual STU III.

PHONE NUMBER
Recipient phone number.

NAME
Recipient name.

INTRVL
Call-back interval.

DAO CODE
Department Agency Organization code.

KEYSET ID
Registration number of recipient's Crypto Ignition Key (CIK)

GEN Broadcast ON/GEN Broadcast OFF

Use these options to toggle the GEN Broadcast ON or OFF. The GEN Broadcast can be used for:

- transmitting data from an SCI to a GENSER machine
- network communications
- exchanging track information between workstations running different versions of UB software (2.1.2.1 and above)

When the broadcast is ON, it will appear in the list of available broadcasts in the BROADCASTS window.

ReMount Global Data

Use this option to access the comms processor data files and load data onto a remote workstation. If the comms processor is reinstalled, or if the alternate comms processor is brought up, use this option on each remote workstation.

If the server is down, or if there is an Ethernet problem, a message indicates the server cannot be found. Click OK to return to the SYSTEM ADMINISTRATOR screen.

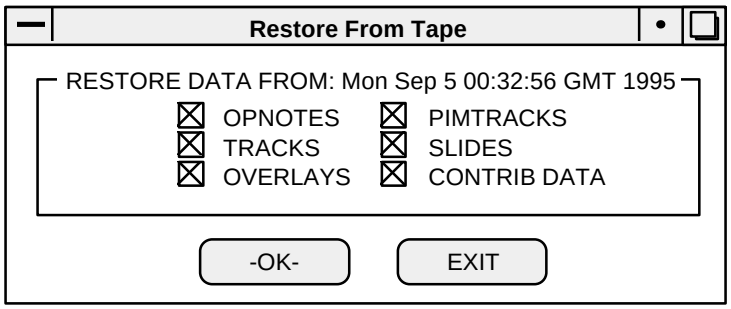
Restore TMS Data

Use this option to restore TMS data to the system. The backup tape must be created using the ARCHIVE TMS DATA option (described in a previous section).

Important:

- Restored data replaces existing data.
- Track data, message logs, and AEN table information must be restored to the server machine. Restoring this data to another machine while the server is running will cause serious problems.
- Data such as overlays or PIM tracks can be restored to *any* machine on the LAN.

To access this window: TMS menu **:** DATABASE menu **:** RESTORE TMS DATA option.



> To restore data:

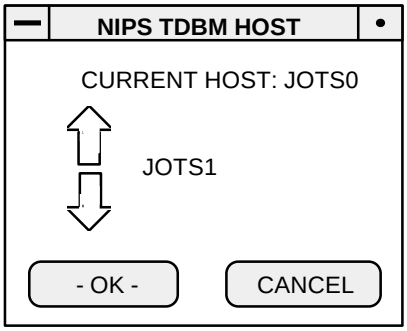
1. **Insert** the backup tape.
2. **Select** RESTORE TMS DATA to display a window similar to Figure 5-8. The DTG stamp indicates when the data was backed up. Only data stored on the tape appears in the window.
3. **Toggle on** any or all of the checkboxes to restore data to the system. A pop-up menu is available with SELECT ALL and UNSELECT ALL options.
4. **Click** OK. When the process is complete, the tape rewinds automatically and the SYSTEM ADMINISTRATOR screen appears.

Set Nips TDBM Host

Use this option to designate the workstation where a user can perform Naval Intelligence Processing System (NIPS) track updates.

- The CP should *not* be a NIPS Tdbm host.
- Tracks can be associated with (or disassociated from) NIPS tracks.
- When updates are received on associated tracks, the NIPS Tdbm automatically updates the NIPS tactical tables.

To access this window: COMMS menu **:** SET NIPS TDBM HOST option.



> To set the NIPS Tdbm Host:

1. **Click** on the arrows until the workstation connected to the NIPS database appears in the window.

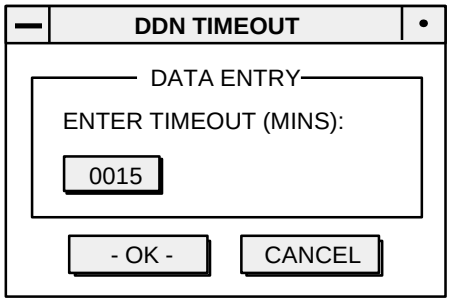
2. **Click** OK to select the host workstation, or click CANCEL to discard the change.

Set WAN DDN Timeout

Use this option to set a time-out period for DDN network operations. The time-out period begins after the DDN channel is started.

If a connection to a remote host fails, or if the time-out period for a receipt expires, a DDN STATUS UNCERTAIN warning is entered in the alert log. If the DDN TIMEOUT knob in the SCREEN ALERT FILTER window is selected, an alert also appears on the tactical display.

To access this window: COMMS menu **:** SET WAN DDN TIMEOUT option.



> To set time-out period:

1. **Enter** the time-out period.
   - Time-out range: 1–3600 minutes.
   - Default value: 15 minutes (0015).
2. **Click** OK to accept the change, or click CANCEL to discard it.

Set WAN UID

This option assigns a three character code which is part of a unique ID (UID) assigned to tracks. The UID is used when the system is in UID correlation mode. The UID is displayed in the track edit window in a non-edit field. It cannot be altered by the user.

- Do not modify the UID unless directed! Using UID Correlation mode without a valid WAN DDN UID can cause serious database problems.
- If a reload is required, use customized installation floppy disk to reinstall the data.

A UID is critical to the integrity of the Data Defense Network's (DDN) contact database; therefore, each wide-area network (WAN) site is assigned a unique address. This address plus the name of each system on the network create a UID for each contact that enters the system.

The UID is formatted as: XXXNNNNNNNNN

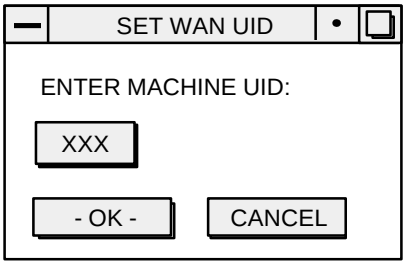
- XXX = the three-character WAN DDN UID

  This is the station identifier that is assigned to a particular system. It marks the tracks added to the DDN from the system.

- NNNNNNNNN = the nine-digit time and date stamp

  The last digit is a counter so two contacts are not assigned the same UID, even if they are added to the track database at the same time. The first three digits are different because the contacts were added at different stations.

To access this window: COMMS **:** SET WAN UID option.



> To change the UID:

1. **Enter** UID.
2. **Click** OK to accept the change, or click cancel to discard it.

TADIL A Menu

The TADIL A menu appears on the System Administrator menubar when the Link-11/TADIL A Admin segment is loaded. The SELECT IMPLEMENTATION option is described in the *Software User's Manual, Link-11/TADIL A.*.

TMS Config

TMS Config is a tool used to define the master server and clients for all track data and message processing for the Track Management System (TMS) and the Universal Communication Processor (UCP). TMS Config provides three types of workstation configuration:

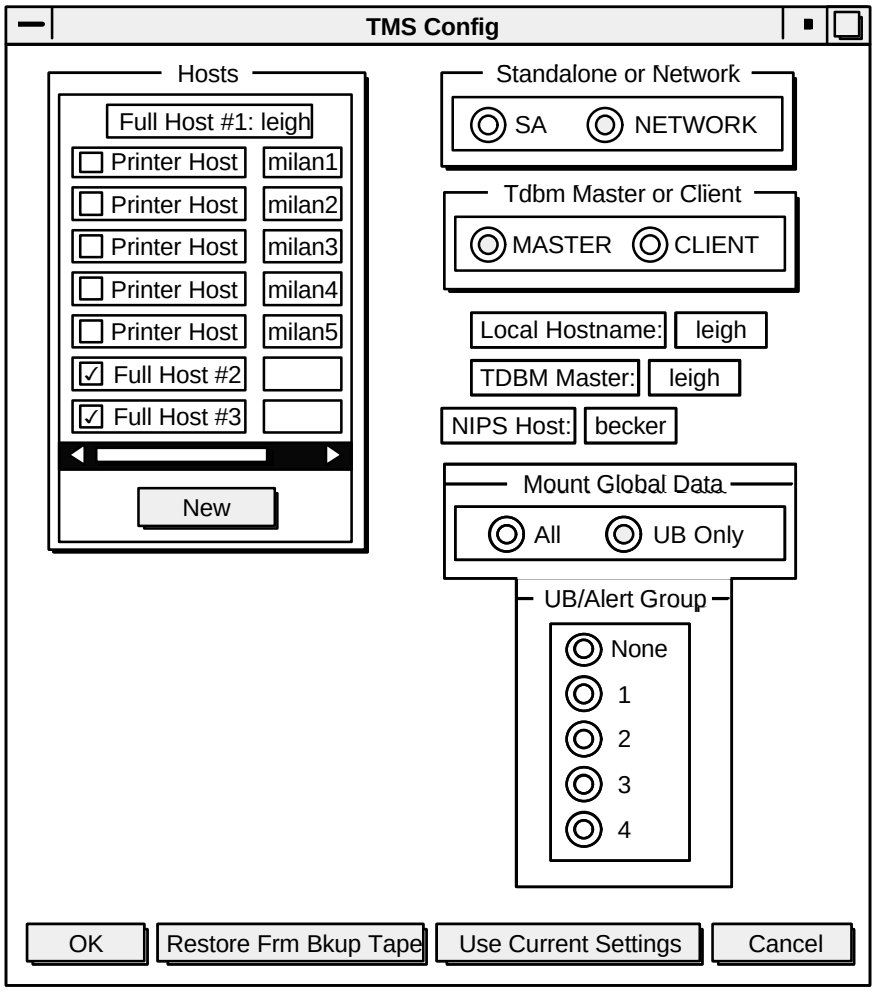
- Standalone
- Single master server with multiple client workstations
- Multiple master servers with client workstations for each on the same physical/logical LAN.

Currently there are 2 fielded Account Groups (JMCIS and C4I) plus one in development (GCCS) that will activate TMS/UCP software. Each of these Account Groups provides pre-set values for TMS/UCP operations.

It is important to determine the following before using TMS Config:

- The type of Account Group that activates TMS/UCP software.
    - The "JMCIS" Account Group (Navy): auto-configures one master server and multiple client workstations (up to a maximum of 30). Using TMS Config in a shipboard JMCIS environment is *not* recommended.
    - The "C4I" Account Group: auto-configures as standalone. When in standalone mode the workstations is it's own master server and ready to process track and message data.
    - The "GCCS" Account Group (when fielded) will be configured the same as C4I Account.
- The desired configuration of the workstations at the site, (i.e. number of master servers, client workstations and standalone workstations).

To access this window: TMS/UCP menu **:** TMS CONFIG option.



About the TMS CONFIG window:

The UB/ALERT GROUP box in this window performs different functions for standalone or network machines.

- On a standalone machine, use the UB/ALERT GROUP to determine the port used for receiving alerts.
    - The default is 1, which allows workstations to receive invalid alerts from each other.
    - To restrict the alerts received on this machine, choose 2, 3, or 4 to set the port to a different number. Each number increases the port number by one.
    - Each standalone machine should have a different alert setting.

- On a network machine, use the UB/ALERT GROUP to create up to four masters with clients for each on a physical, logical LAN.
    - A physical, logical LAN is group of machines on the same physical LAN whose IP addresses are identical in the first three sets of numbers and each machine in the group is identified by the last set of unique numbers.
    - For example, all machines on the physical LAN have an IP address of 194.84.121.xxx, where "xxx" is a unique number for each machine.

> To configure a standalone machine:

Note: The window is in STANDALONE mode when it opens.

1. Choose SA in the STANDALONE OR NETWORK box.
2. If more than one workstation on the LAN is standalone, select one of the alert groups (1,2,3 or 4) in the UB/ALERT GROUP box.
    - **Important:** There is no auto-detect capability to determine which alert group is already selected on another standalone machine.
    - Assign a unique number to each machine.
3. Click OK to accept the changes, or CANCEL to discard.
4. Select NO in the BACKUP YOUR SETTING TO TAPE warning window. Select OK in all other warning windows.
5. Reboot the system for the changes to take effect. (Use REBOOT from the HARDWARE menu.)

> To configure one master with multiple clients on a network:

Note: The window is in STANDALONE mode when it opens.

1. Select NETWORK in the STANDALONE OR NETWORK box.
2. Select MASTER in the TDBM MASTER OR CLIENT box if the machine is the master. (Always set the master machine before setting clients.) Select CLIENT if the machine is a client.
3. Enter the name of the Tdbm master in the TDBM MASTER field.
    - On the master machine, the name of the workstation is automatically entered in the TDBM MASTER field when MASTER is selected.

- On a client machine, enter the name of the master in the TDBM MASTER field. Delete current entry before typing new name.
- Press RETURN for the new name to be accepted. It should appear in the FULL HOST #1 field.

4. If the NIPS segment is loaded, enter the NIPS server name in the NIPS HOST field.

5. Configure master/client groups in the UB/ALERT GROUPS box:

   - Choose NONE for a single master and all other machines on the LAN as clients.
   - To configure more than one master with clients on the LAN, on each master machine, assign a unique number (1-4) and add client machines for that master in the HOSTS list. There is no auto-detect capability to determine which UB group is already selected on another standalone machine.
   - Save the master machine configuration to tape and use RESTORE FRM BKUP TAPE to configure client machine (see steps 8 and 9).

5. Click NEW in the HOSTS box to add client machine names to the list. (All machine names and IP addresses must be in the machine's hosts list. Use the EDIT LOCAL HOSTS option to add machines to this list.)

6. Enter names of printers that are connected to the LAN in the PRINTER HOST fields.

7. Click OK to accept the changes, or CANCEL to discard.

8. At the prompt, insert a tape and click OK to save the settings to a backup tape.

9. On each client machine, insert this backup tape and click RESTORE FRM BKUP TAPE to automatically enter the master machine settings on the client machine. (Note: Each client machine must be configured *exactly* the same as the master machine.)

10. Reboot the machine for changes to take effect. (Use REBOOT from the HARDWARE menu.)

> To configure a client machine on a network:

1. Select CLIENT in the TDBM MASTER OR CLIENT box. (Always set the master machine before setting clients.)

2. On each client machine, insert the backup tape from the client's master machine and click RESTORE FRM BKUP TAPE to automatically enter the master machine settings.

    - **Important**: Each client machine must be configured *exactly* the same as the master machine.
    - If settings are entered manually, enter in the same order as for the master machine. Follow steps 2-6 in the previous section.
    - When entering the master machine name in the TDBM MASTER field, press [RETURN] to accept the name. The machine name should appear in the FULL HOST #1 field.

3. In the MOUNT GLOBAL DATA box, choose ALL to access all data in the global data file directory of the master machine or choose UB ONLY to access only TMS/UCP data.

4. Click OK to accept the configuration, or CANCEL to discard.

5. At the prompt, insert a tape and click OK to save the settings to a backup tape.

6. Reboot the machine for changes to take effect. (Use REBOOT from the HARDWARE menu.)

TMS CONFIG Window Buttons

USE CURRENT SETTINGS—recalls the previous settings for all fields.

RESTORE FRM BKUP TAPE—enters settings in all fields from a backup tape.

TMS CONFIG Window Fields

FULL HOST #1:
Name of the master machine.

PRINTER HOST
Printer host name. Checkbox is OFF.

FULL HOST #n
Client machine names. Checkbox is ON.

SA
Designates this machine as a standalone machine.

NETWORK
Designates this machine as a network machine.

MASTER
Designates this machine as the Tdbm master for a network.

CLIENT
Designates this machine as a client to the Tdbm master.

LOCAL HOSTNAME
Name of this workstation. This field cannot be edited.

TDBM MASTER
Name of the Tdbm master for the network. This field can be edited only if CLIENT is selected.

NIPS HOST
Name of Naval Intelligence Processing System (NIPS) host machine. (NIPS segment must be loaded.)

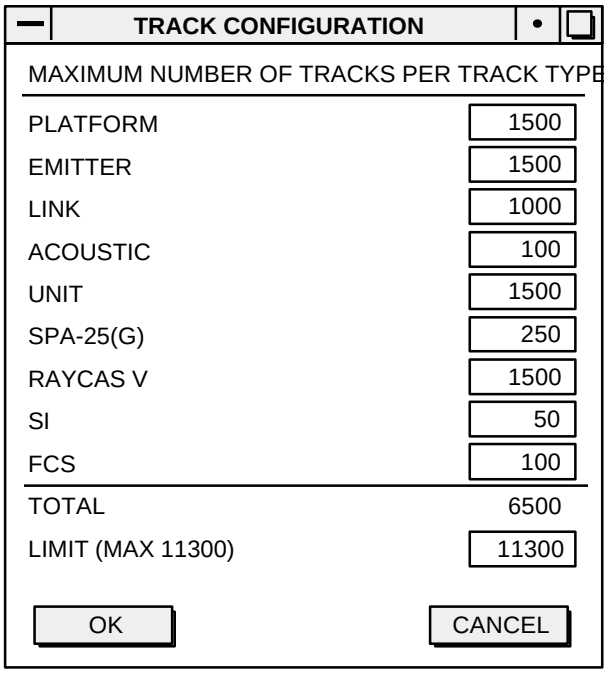
MOUNT GLOBAL DATA
Configures client workstations to access all data files or only TMS/UCP data in the global data file directory of the master server or.

UB/ALERT GROUP
Determine alert port for a standalone machine, or configure master and client groups on a physical, logical LAN.

Track Database Reconfig

Use this option to designate the maximum number of tracks allowed in the system for each track type, up to 11,300 total tracks.

To access this window: TDBM menu **:** HARDWARE cascading menu **:** TRACK DATABASE RECONFIG option.



> To set track database sizes:

1. Enter a limit for total tracks allowed in the system, no more than11,300.
2. Enter maximum number of tracks for each track type.
3. Click OK to save the changes, or CANCEL to discard.
4. Reboot the machine for changes to take effect.

TRACK CONFIGURATION Window Fields

TRACK TYPE

Number of tracks allowed in the system for each track type: Platform, Emitter, Link, Acoustic, Unit, SPA-25(G), RAYCAS V, SI, and FCS.

TOTAL
Number of tracks entered for all track types.

LIMIT
Maximum number of all track types allowed in the system.

Notes

Communications

Default Communications Channels

These channels are installed as the master default list of comms channels.

TTY DEVICE	*ASSIGNED TO*
A	Serial
B	TRE-OTG
C	GFCP/Terminal Control
C0	Link-11 (PED, PIH)
C1	OTCIXS-TTY
C2	OTCIXS
C3	TADIXS
C4	Owntrack NAV Interface
C5	Link-14
C6	HIT-BCST
C7	FLT-BCST-1
D	GENSERPOST
D0	(none)
D1	TADIXS TTY
D2	DTC
D3	Remote Link-11 (future)
D4	Remote Link-11 RXA (future)
D5	Remote Link-11 RXB (future)
D6	FLT-BCST-2
D7	(none)
NTDS0	ACDS POFA Link-11-ACT WRN-6 WSN-5 SDMS

Important:

- C*n* and D*n* channel assignments are valid only when 8-port MUX boards are used with HP-UX 9.07 OS.
- NTDS*n* channel assignments are valid only when NTDS boards are used with HP-UX 9.07 OS.

If settings have been modified (device settings, protocol parameters, or both) it is possible to return to the original system defaults. However, information pertaining to any new channels is removed. The current list can be saved to recall later.

> To save the current settings:

1. Select DEFAULTS from the COMMUNICATIONS window pop-up menu to open the DEFAULTS window.

2. Enter a name in the SAVED NAME field and click SET.

> To recall these settings:

1. Open the DEFAULTS window.

2. Highlight the name assigned to the saved settings and click GET.

3. The system stops and restarts all channels.

> To reset channels to the original system defaults

- Select MASTER DEFAULT from the COMMUNICATIONS window pop-up menu.

  The system stops and restarts all channels.

  Remember, incoming messages could be lost during the time it takes to accomplish this task (approximately 1–2 minutes).

Troubleshooting Communications Problems

If messages are not being received or transmitted, the problem may be solved by checking the following hardware and software components. Correcting every communications problem is beyond the scope of this document, however some common trouble areas include:

- Connections between communications hardware and the workstation are established incorrectly.
- External communications devices are set incorrectly.
- Options that affect communications are set incorrectly.

NOTE: Within this section, "COMMS MENU" refers to the menu on the SYSTEM: DEFAULT MODE screen, *not* the System Administrator screen.

Hardware Problems

Check the following:

- Communications antennas must be positioned to the proper azimuth.
- Radios must be up and running, with everything set correctly.
- Modems must be running properly.
- Cryptologic devices must be loaded and set correctly.
- Devices connected to the workstation must be operational and set correctly.
- Connections must be tight.
- Check data converters.
- If the connection is serial, test the line with a breakout box.

  Connect the breakout box to the machine, then to the comms line.

  Verify signals are being provided by both sides without conflict. For example, the machine and the comms line could both have a signal on pin 2.
- If a properly configured comms channel is connected directly to a crypto/radio, and data results, check for an improper crypto hardware or crypto key.

Software Problems

Check the following:

- Comms channels must be running. Otherwise, incoming messages could be lost and outgoing message could overload the buffer.
- Use incoming message logs and outgoing message logs to verify that messages are entering and leaving the system.

  Messages that have not been transmitted display as dots in the MSG TOT field (outgoing message logs).
- Comms channel parameters must be set correctly.

  The machine associated with the comms channel must be the same machine to which the channel is connected.

  The port (device) listed for the comms channel must be the same port to which it is connected.
- If messages are garbled, check the comms channel parameters such as baud rate, stop bits, etc.
- If messages are received but tracks are not displayed, check:

  INPUT MSG FILTERS

  INPUT GEO FILTERS

  Applicable options in the PLOT CONTROL menu
- If the channel is a serial interface, toggle on the CRYPTO PHASE checkbox to make sure messages are handled properly.

  This checkbox is available for systems using the KG-84 encryption device (usually operating at 75 baud).

Specific Channels and Interfaces

Troubleshooting suggestions for the following channels are addressed in this section:

- Link-11
- MDX
- Network

Link-11 Channel

The system receives Link-11 data via a serial interface from an EDO box. (Though the EDO box also has an IEEE-488 interface, the system uses only the serial.) Another alternative is an Indian Head serial interface.

The EDO box passively taps the transmit and receive side of Link-11. Link-11 can be run in one of three modes:

- NCS—the ship is the Link-11 controller
- PKT—the ship is a Link-11 picket unit
- RS—the ship is radio silent

The system receives Link-11 data from all participating units (PUs), other than Owntrack, if Link-11 and its related components are operational. These components include modem, crypto, radio, and antenna.

The system receives Owntrack Link-11 data under the following conditions:

- The Owntrack NTDS must be operational.
- Link-11 must be in the NCS or PKT mode.

The system not receiving data from PUs:

1. **Contact** the Track Supervisor or Tactical Information Controller (TIC) to verify that the Link-11 components are operational.

2. **Check** the error lights on the EDO box. If an error light is on, the EDO box is preventing the Link-11 data from reaching the system.

3. **Check** the Link-11 comms channel in the system. (For more information, see *Troubleshooting Software Problems*, described in this chapter.)

The system not receiving data from Owntrack:

1. **Make sure** the Owntrack NTDS is operational.

2. **Check** the Link-11 control panel settings. Owntrack Link-11 data will be received only if the unit is in NCS or PKT mode, *not* RS.

MDX

The MDX interface provides point-to-point data communications—specifically, transmitting track information from one designated site to another.

If the interface is not transmitting data, check the following:

- MDX patch Version 5 is loaded.
- The channel is configured properly.
- The route has been established between sites.
- Exact site host names appear in the host table.

- The transmit and receive port designations do not conflict with existing TCP port numbers in the /etc/services file.
- The values for transmitting port at one site match the values for the receiving port at the other site.

Network

If the interface is not transmitting or receiving data, check the following:

- Confirm the DDN Host Table has a correctly entered UHID. The UHID for both sites must match.
- The other site has a network channel configured and activated.

Broadcasts

To troubleshoot a particular broadcast:

- Open the status window for the broadcast. (Broadcast must be ON; use the WINDOW pop-up option.)
- Open the window for the outgoing comms channel.
- Compare message activity.
- Ensure the Commands in the "TO:" fields in the default header are the same as those listed in the Auto-Forward Table.